CLAIMS

1. A packet-switched data communication system comprising:

a network interface configured to couple to a packet-switched network;

a communication session module coupled to the network interface and configured to establish a communication session with a telecommunication device through the packet-switched network;

a communication processing module coupled to the network interface and configured to receive real-time communication data, arrange the communication data in a sequence of packets, and send the sequence of packets to the network interface; and

an encryption module coupled to the communication processing module and configured to selectively encrypt the received communication data in response to an encryption indication received via the network interface.

2. The system of claim 1 wherein the encryption indication is indicative of an encryption request initiated by a user of the telecommunication device.

3. The system of claim 1 wherein the encryption indication is the received real-time communication data being encrypted.

4. The system of claim 1 wherein the communication session module is configured to establish communication sessions with multiple telecommunication devices through the network, and wherein the communication processing module is further configured to provide a security indication to at least a first of the telecommunication devices through the network interface indicative of whether communications from the network interface toward a second of the telecommunication devices is secure.

5. The system of claim 4 wherein the security indication is indicative of whether communications are encrypted.

6. The system of claim 4 wherein the system includes the first of the telecommunication devices, the first telecommunication device being coupled to the network interface and configured to store a public encryption key and to provide the public encryption key to the encryption module.

7. The system of claim 6 wherein the first telecommunication device includes a secure communication selector and is configured to provide the device encryption key to the encryption module in response to actuation of the secure communication selector.

8. The system of claim 7 wherein the first telecommunication device further includes a docking port for receiving a portable communication device, the first telecommunication device being further configured to provide an encryption indication to the docking port to cause the portable communication device received by the docking port to display an indication that communications from the first telecommunication device to the network interface are encrypted.

9. The system of claim 7 wherein the first telecommunication device further includes a docking port for receiving a portable communication device, the first telecommunication device being further configured to process the security indication and to provide the processed security indication to the docking port to cause the portable communication device received by the docking port to display an indication that communications from the network interface to at least the second telecommunication device are secure.

10. A telecommunication device for communication with a communication endpoint device via a packet-switched network, the telecommunication device comprising, in combination:

an interface configured to couple to the network;

a microphone for receiving sound signals;

a speaker for providing sound signals corresponding to signals received via the interface from the network; and

a data processing module coupled to the interface and configured to receive data from the interface, process the received data, and to provide an indication for causing a display at least temporarily associated with the telecommunications device to display an indication of whether communications between the telecommunications device and the endpoint device are secure.

11. The telecommunication device of claim 10 further comprising a device encryption module coupled to the interface and configured to store a public device encryption key and to provide the public device encryption key to the interface for transmission to the endpoint device.

12. The telecommunication device of claim 11 further comprising a secure communication selector and is configured to provide the public device encryption key to the interface in response to actuation of the secure communication selector.

13. The telecommunication device of claim 12 further comprising a docking port for receiving a portable communication device, the device encryption module being further configured to provide an encryption indication to the docking port to cause a portable communication device received by the docking port to display an indication that communications from the telecommunication device to the endpoint device are encrypted.

14. The telecommunication device of claim 13 wherein the data processing module is further configured to receive a security indication received by the interface and to provide the encryption indication to the docking port in response to receiving the security indication.

15. A method of providing secure communications between a plurality of communication units, the method comprising:

conveying a first communication from a first communication unit to a second communication unit, the first communication being unsecure;

determining whether a user-actuated selector to secure communications from the first communication unit to at least the second communication unit is currently actuated; and

conveying the second communication from the first communication unit toward the second communication unit in a secure manner if the selector is currently actuated.

16. The method of claim 15 further comprising encrypting the second communication if the selector is actuated, wherein conveying the second communication comprises conveying the second, encrypted, communication.

17. The method of claim 16 wherein the second communication unit is a control unit configured to relay communications from the first communication unit to a plurality of third communication units, the method further comprising:

receiving at the second communication unit, an indication that the second communication is encrypted;

decrypting the second communication to produce a decrypted second communication;

encrypting the decrypted second communication in accordance with encryption

keys, if available, associated with the third communication units to produce re-encrypted second communications; and

conveying the re-encrypted second communications from the second communication unit to the respective third communication units.

18. The method of claim 17 further comprising:

providing security indicia to the first communication unit indicative of to which third communication units the second communication unit transmits re-encrypted second communications; and

displaying, on a display associated with the first communication unit, whether communications between the second communication unit and the respective third communication unit are secure.

19. The method of claim 15 further comprising displaying on a display associated with the first communication unit that communication between the first communication unit and the second communication unit is secure.

20. The method of claim 15 wherein the second communication unit is a control unit configured to relay communications from the first communication unit to at least a third communication unit, the method further comprising:

receiving, at the second communication unit, an indication that the selector is actuated; and

conveying the second communication from the second communication unit to the third communication unit in a secure manner.

21. A communication system for bridging communication sessions into a conference call, the system comprising:

at least one network interface configured to couple to a packet-switched network;

a session module coupled to the at least one network interface and configured to establish communication sessions with a plurality of conference-participating devices through the at least one network interface via the packet-switched network;

a signal-mixing module coupled to the session module and configured to mix audio streams from the conference-participating devices and to supply mixed streams toward the conference-participating devices; and

security means, coupled to the at least one network interface and to the signal-mixing module, for securing communications from the signal-mixing module in response to a secure communication indication.

22. The system of claim 21 wherein the secure communication indication is a security signal received via the at least one network interface from a conference-participating device.

23. The system of claim 21 wherein the security means is configured for notifying at least one of the conference-participating devices to which, if any, of the conference-participating devices the mixed signals are sent in a secure manner.

24. The system of claim 21 wherein the securing communications includes encrypting the mixed streams.

25. The system of claim 21 wherein the securing communications includes directing the mixed signals to limited-access secure lines via the at least one network interface.

26. The system of claim 21 wherein the security means is configured for decrypting incoming encrypted audio streams.

27. The system of claim 26 wherein the secure communication indication is an indication that an incoming audio stream is encrypted.

28. A telecommunications station for transducing at least one of sound and video signals to outgoing electronic signals and sending the outgoing electronic signals over a telecommunications line and for transducing incoming electronic signals received via the telecommunications line to incoming media signals being at least one of incoming sound signals and incoming video signals, the telecommunications station comprising in combination:

an interface module configured to establish a communication session between the station and a communication endpoint over the telecommunications line;

secure session means for detecting operator request for at least secure outgoing communications over the telecommunications line and providing an indication for secure outgoing communications; and

an encryption module coupled to the secure session means and configured to encrypt outgoing electronic signals in response to the indication for secure outgoing communications provided by the secure session means.

29. The station of claim 28 wherein the secure session means is also for detecting an endpoint request, received via the telecommunications line, for at least secure incoming communications and providing an indication for secure incoming communications, and wherein the encryption module is further configured to decrypt incoming electronic signals in response to the indication for secure incoming communications provided by the secure session means.

30. The station of claim 29 wherein the indication for secure incoming communications and the indication for secure outgoing communications are the same indication.

31. The station of claim 28 further comprising means for indicating secure status of communications from the station via the telecommunications line.

32. The station of claim 31 wherein the means for indicating secure status comprises means for receiving participant-security indications via the telecommunications line indicative of whether communications to each of multiple conference-call participants are secure.

33. The station of claim 32 wherein the means for indicating secure status indicates secure status of a conference-call only if the participant-security indications indicate that communications to all of the conference-call participants are secure.